



The Latest Scams Circulating the Consumer World.



APRIL 2011

SMARTPHONE PICTURE UPLOADS POSE SECURITY RISKS

The Hook

Using the incredible capabilities of their smart phones, many owners are tempted to use the geotagging capabilities to post pictures of their children or friends on the internet using the services of social networking sites like Facebook and Twitter. However, by doing this they are unwittingly exposing their children to threats of kidnapping or abuse by showing their exact location at various times of the day.



The Whole Story

A recent investigation by an NBC news affiliate in Kansas City has uncovered this very scary potential for those parents who post photos on the internet of their children taken by smart phones. The risk comes from the fact that these smart phones, through their GPS capability, enable geotagging of photographs that are later uploaded to the internet on websites such as Facebook, Craig's List, Twitter, and Photobucket. The full news story and investigation can be seen at www.youtube.com/watch?v=N2vARzvWxwY.

Using free, easily available software, smart phones leave a highly visible trail of their user's whereabouts. The software can tell a person exactly where the phone is at any given time a photo was taken and later uploaded. The software can translate geotagged photos uploaded and linked from popular websites into exact maps, tracing routes of travel between photos.

The Lesson

The investigative report referred to above shows how threatening a seemingly innocent snapshot can be when posted online from a smart phone. In the test conducted on photos taken by a newsroom staffer of her daughter, the investigative reporter and police officer Mark Chudik were able to obtain the address of the young girl's home, locate her day care center, her favorite fast food shop, and the specific area of the park where she frequently plays. "The fact that they found the bedroom is terrifying," the mother said. The investigative team also searched online servers by local cities, and thereby created a menu of nearby children and their locations. Police officer Chudik called the hidden smart phone data today's biggest risk online.

To prevent this kind of information from being publicly available online, simply disable the geotagging capabilities of your smart phone before photographs are taken and posted online. The website <http://icanstalku.com/how.php> reposts pictures from unwitting Twitter users in real time, translating their photos into actual addresses. More importantly, the website gives specific instructions on how to deactivate geotagging on the iPhone, Blackberry with GPS, Google Android, and Palm WebOS. Be smart and doubly safe... deactivate the geotagging capability on your smart phone.